

§ 105.260

33 CFR Ch. I (7–1–10 Edition)

another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired facility employees may be granted the access provided for in paragraph (a) of this section if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The facility owner or operator or the Facility Security Officer (FSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The facility owner or operator or the FSO enters the following information on the new hire into the Coast Guard's Homeport website (<http://homeport.uscg.mil>):

- (i) Full legal name, including middle name if one exists;
- (ii) Date of birth;
- (iii) Social security number (optional);
- (iv) Employer name and 24 hour contact information; and
- (v) Date of TWIC enrollment.

(3) The new hire presents an identification credential that meets the requirements of §101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the facility owner or operator or FSO have not been informed by the cognizant COTP that the new hire poses a security threat; and

(5) There would be an adverse impact to facility operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a FSO, or any individual being hired to perform facility security duties.

(d) The new hire may not begin working at the facility under the provisions of this section until the owner, operator, or FSO receives notification, via Homeport or some other means, the

new hire has passed an initial name check.

[USCG-2006-24196, 72 FR 3584, Jan. 25, 2007]

§ 105.260 Security measures for restricted areas.

(a) *General.* The facility owner or operator must ensure the designation of restricted areas in order to:

- (1) Prevent or deter unauthorized access;
- (2) Protect persons authorized to be in the facility;
- (3) Protect the facility;
- (4) Protect vessels using and serving the facility;
- (5) Protect sensitive security areas within the facility;
- (6) Protect security and surveillance equipment and systems; and
- (7) Protect cargo and vessel stores from tampering.

(b) *Designation of Restricted Areas.* The facility owner or operator must ensure restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner or operator may also designate the entire facility as a restricted area. Restricted areas must include, as appropriate:

- (1) Shore areas immediately adjacent to each vessel moored at the facility;
- (2) Areas containing sensitive security information, including cargo documentation;
- (3) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and
- (4) Areas containing critical facility infrastructure, including:
 - (i) Water supplies;
 - (ii) Telecommunications;
 - (iii) Electrical system; and
 - (iv) Access points for ventilation and air-conditioning systems;
- (5) Manufacturing or processing areas and control rooms;
- (6) Locations in the facility where access by vehicles and personnel should be restricted;
- (7) Areas designated for loading, unloading or storage of cargo and stores; and

(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

(c) The owner or operator must ensure that all restricted areas have clearly established security measures to:

(1) Identify which facility personnel are authorized to have access;

(2) Determine which persons other than facility personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply;

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security;

(7) Control the entry, parking, loading and unloading of vehicles;

(8) Control the movement and storage of cargo and vessel stores; and

(9) Control unaccompanied baggage or personal effects.

(d) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Assigning personnel to control access to restricted areas;

(4) Verifying the identification and authorization of all persons and all vehicles seeking entry;

(5) Patrolling or monitoring the perimeter of restricted areas;

(6) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry or movement within restricted areas;

(7) Directing the parking, loading, and unloading of vehicles within a restricted area;

(8) Controlling unaccompanied baggage and or personal effects after screening;

(9) Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading; and

(10) Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.

(e) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas;

(2) Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices;

(3) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(4) Restricting parking adjacent to vessels;

(5) Further restricting access to the restricted areas and movements and storage within them;

(6) Using continuously monitored and recorded surveillance equipment;

(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas; or

(8) Establishing and restricting access to areas adjacent to the restricted areas.

(f) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in

§ 105.265

33 CFR Ch. I (7-1-10 Edition)

their approved FSP. These additional security measures may include:

- (1) Restricting access to additional areas;
- (2) Prohibiting access to restricted areas, or
- (3) Searching restricted areas as part of a security sweep of all or part of the facility.

§ 105.265 Security measures for handling cargo.

(a) *General.* The facility owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to:

- (1) Deter tampering;
- (2) Prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator;
- (3) Identify cargo that is approved for loading onto vessels interfacing with the facility;
- (4) Include cargo control procedures at access points to the facility;
- (5) Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;
- (6) Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;
- (7) Ensure the release of cargo only to the carrier specified in the cargo documentation;
- (8) When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and
- (9) Create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of measures to:

- (1) Unless unsafe to do so, routinely check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling operations for evidence of tampering;

- (2) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;

- (3) Screen vehicles; and

- (4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

- (1) Conducting check of cargo, containers or other cargo transport units, and cargo storage areas within the facility for evidence of tampering;

- (2) Intensifying checks, as appropriate, to ensure that only the documented cargo enters the facility, is temporarily stored there, and then loaded onto the vessel;

- (3) Intensifying the screening of vehicles;

- (4) Increasing frequency and detail in checking of seals and other methods used to prevent tampering;

- (5) Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures;

- (6) Increasing the frequency and intensity of visual and physical inspections; or

- (7) Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.

(d) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

- (1) Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels;

- (2) Being prepared to cooperate with responders and vessels; or